



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/240,934	01/29/1999	YAIR BARTAL	2-5-7	7975

7590 09/05/2002

RYAN, MASON & LEWIS, LLP  
1300 Post Road  
Suite 205  
Fairfield, CT 06430

EXAMINER
----------

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/05/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

PRH

**Office Action Summary**

Application No.

09/240,934

Applicant(s)

BARTAL ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE \_\_\_\_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on 09 May 2002.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☐ Claim(s) 1-8 and 29-38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) 1-8, 29-35 and 38 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_
- 4) ☐ Interview Summary (PTO-413) Paper No(s) \_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_

**NORMAN M. WRIGHT**  
**PRIMARY EXAMINER**

Art Unit: 2131

## DETAILED ACTION

### *Response to Arguments*

1. Applicant's arguments with respect to claims 1-8, 29-35, and 38 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reid et al in view of Arrow et al.

As per claim 29, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col. 2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access

Art Unit: 2131

control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page. The teachings of Reid et al are silent in disclosing of each of the roles may be assigned to hosts independently of a topology of the network. This feature is disclosed by Arrow et al wherein it is disclosed of an access control role (policy) which specifies that communications between non-members (independent hosts of the topology) of a VPN and members of a VPN are not allowed to pass through a particular VPN unit (col. 15, lines 63-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a policy independent of the topology of the network so that communications can exist either for members and non-members. Arrow et al recites motivation for use of this feature by reciting that the access control rules (policy) specify which type of communications are allowed to pass (col. 15, lines 61-62). It would have been obvious to apply this feature to the teachings of Reid et al as a means allowing communications between regions whereby the particular hosts may apply to different regions.

4. Claims 1-8,29-35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reid et al in view of Grennan in further view of Arrow et al.

As per claim 1, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col.

Art Unit: 2131

2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page. The teachings of Reid et al fail to disclose of generation of a configuration file for a firewall. It is disclosed by Grennan of setting up (generating) a configuration file for a firewall (section 4.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate the how the firewall functionality is to be performed. Although Reid et al is silent on the use of a configuration file, it is essential that a configuration file exists in the teachings since it is notoriously well known that configuration files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

The teachings of Reid et al are silent in disclosing of each of the roles may be assigned to hosts independently of a topology of the network. This feature is disclosed by Arrow et al wherein it is disclosed of an access control role (policy) which specifies that communications between non-members (independent hosts of the topology) of a VPN and members of a VPN are not allowed to pass through a particular VPN unit (col. 15, lines 63-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a policy independent of the topology of the network so that communications can exist

Art Unit: 2131

either for members and non-members. Arrow et al recites motivation for use of this feature by reciting that the access control rules (policy) specify which type of communications are allowed to pass (col. 15, lines 61-62). It would have been obvious to apply this feature to the teachings of Reid et al as a means allowing communications between regions whereby the particular hosts may apply to different regions.

As per claims 2 and 31, Reid et al shows a plurality of firewalls in Figures 1a and 1b which are in defined regions (assignment of roles)(col. 1, lines 54-56). Grennan is relied upon for disclosing the use of a configuration file (section 4.2).

As per claim 3, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col. 2, lines 8-17). The network capabilities are dictated for the services of the regions (col. 20, lines 39-44).

As per claims 4, 5, 32, and 33, Reid et al discloses of an interface card (belonging to respective hosts), VPNs, groups of VPNs, or any groupings thereof to exist in the regions (assignment of roles)(col. 5, lines 3-13).

As per claims 6 and 34, it is disclosed by Reid et al of providing policies for a plurality of regions to restrict communications to and from each of the regions. The teachings of Reid et al

Art Unit: 2131

are silent on providing a visual representation of the structure of the hosts in the network. The examiner hereby asserts that it would have been obvious to in means for including a visual representation of the of the structure of the hosts in the network. It is suggestive of providing a visual representation of the structure of the hosts in the network where it is taught by Reid et al that a visual means is provided by which access control (rules of the configuration file) can be defined (col. 7, lines 8-12 and 24-27) and also disclosed of GUI is used as a means to dictate how the rules are implemented (col. 8, lines 33-36) wherein the representation of the hosts in the network can be examined since there exists groupings of networks and VPNs in different regions wherein a specific security policy is applied thereto (col. 4, line 66 through col. 5, line 5). By providing a visual representation of the topology of the hosts in the network, the hosts belonging to a particular region can be easily identified and have certain access control rules applied as suggested by Reid et al.

As per claim 7, it is disclosed by Reid et al that a visual means (representation) is provided by which access control (rules of the configuration file) can be defined (col. 7, lines 8-12 and 24-27).

As per claims 8 and 35, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of

Art Unit: 2131

roles)(col. 2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page. The teachings of Reid et al fail to disclose of a compiler for generation of a configuration file for a firewall. It is disclosed by Grennan of setting up (generating) a configuration file for a firewall and compiling (by means of a compiler) the kernel (section 4.2, 5.1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a compiler for generating a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate the how the firewall functionality is to be performed. Although Reid et al is silent on the use of a compiler for generation of a configuration file, the teachings of Reid et al are suggestive of compiling wherein it is disclosed of ACLs (rules) used by the kernel for building, modifying, deleting, and querying the rules (col. 8, lines 20-23) which would need compiled. It is essential that a compiler for generating a configuration file exists in the teachings since it is notoriously well known that compiling the configuration files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

The teachings of Reid et al are silent in disclosing of each of the roles may be assigned to hosts independently of a topology of the network. This feature is disclosed by Arrow et al wherein it is disclosed of an access control role (policy) which specifies that communications



Art Unit: 2131

between non-members (independent hosts of the topology) of a VPN and members of a VPN are not allowed to pass through a particular VPN unit (col. 15, lines 63-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a policy independent of the topology of the network so that communications can exist either for members and non-members. Arrow et al recites motivation for use of this feature by reciting that the access control rules (policy) specify which type of communications are allowed to pass (col. 15, lines 61-62). It would have been obvious to apply this feature to the teachings of Reid et al as a means allowing communications between regions whereby the particular hosts may apply to different regions.

The teachings of Reid et al are silent on the use of a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code. The examiner hereby asserts that it would have been obvious that the teachings of Reid et al comprise a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code in order for the teachings to be performed as disclosed. The software program (computer readable code) and necessary hardware (processor and memory) to perform the necessary tasks are notoriously known to one of skill in the art as an essential part of computing. It is obvious that the teachings of Reid et al exist in the form of a software program (computer readable code) and are utilized by the hardware, namely stored in memory and a processor interprets, processes, and performs the task of providing

Art Unit: 2131

policies for a plurality of regions to restrict communications to and from each of the regions as enforced by a firewall.

As per claim 30, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The teachings of Reid et al fail to disclose of translating of a configuration file for a firewall. It is disclosed by Grennan of setting up a configuration file for a firewall and compiling the kernel (section 4.2, 5.1). It is inherent that the configuration file would have been translated into a language that is used by the computer system since it is notoriously well known that different computing systems use different types of operating systems and there exists a need to convert a program into a language that is interpretable by a computing system using a different language from another. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a compiler for generating a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate the how the firewall functionality is to be performed. Although Reid et al is silent on the use of a compiler for generation (translating) of a configuration file, the teachings of Reid et al are suggestive of compiling wherein it is disclosed of ACLs (rules) used by the kernel for building, modifying, deleting, and querying the rules (col. 8, lines 20-23) which would need compiled. It is essential that a compiler for generating a configuration file in the format that is to be used by a system exists in the teachings since it is notoriously well known that compiling the configuration

Art Unit: 2131

files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

As per claim 38, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col. 2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page. The teachings of Reid et al fail to disclose of generation of a configuration file for a firewall. It is disclosed by Grennan of setting up (generating) a configuration file for a firewall (section 4.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate t\*-3.he how the firewall functionality is to be performed. Although Reid et al is silent on the use of a configuration file, it is essential that a configuration file exists in the teachings since it is notoriously well known that configuration files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of

Art Unit: 2131

Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

The teachings of Reid et al are silent in disclosing of each of the roles may be assigned to hosts independently of a topology of the network. This feature is disclosed by Arrow et al wherein it is disclosed of an access control role (policy) which specifies that communications between non-members (independent hosts of the topology) of a VPN and members of a VPN are not allowed to pass through a particular VPN unit (col. 15, lines 63-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a policy independent of the topology of the network so that communications can exist either for members and non-members. Arrow et al recites motivation for use of this feature by reciting that the access control rules (policy) specify which type of communications are allowed to pass (col. 15, lines 61-62). It would have been obvious to apply this feature to the teachings of Reid et al as a means allowing communications between regions whereby the particular hosts may apply to different regions.

The teachings of Reid et al are silent on the use of a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code. The examiner hereby asserts that it would have been obvious that the teachings of Reid et al comprise a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code in order for the teachings to be performed as disclosed. The software program (computer readable code) and necessary hardware

Art Unit: 2131

(processor and memory) to perform the necessary tasks are notoriously known to one of skill in the art as an essential part of computing. It is obvious that the teachings of Reid et al exist in the form of a software program (computer readable code) and are utilized by the hardware, namely stored in memory and a processor interprets, processes, and performs the task of providing policies for a plurality of regions to restrict communications to and from each of the regions as enforced by a firewall.

### *Conclusion*

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2131

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications: (703) 746-7238;


for Official Communications: (703) 746-7239;

for Non-Official Communications: (703) 746- 7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

CR

August 22, 2002

  
NORMAN M. WRIGHT  
PRIMARY EXAMINER  
AL2131